UNODC tackling cybercrime in support of a safe and secure AP-IS

Mr. Alexandru CACIULOIU
Cybercrime Project Coordinator
South East Asia and the Pacific

Second session of the Asia-Pacific Information Superhighway (AP-IS) Steering Committee
WHAT IS CYBERCRIME?

“offenses ranging from criminal activity against data to content and copyright infringement” (Council of Europe’s CC Treaty)

United Nations refers to acts of fraud, forgery and unauthorized access

“...unlawful acts wherein the computer is either a tool or a target or both.”.

Categories of Cybercrime:

**Cyberpiracy** - using cyber-technology in unauthorized ways to:

**Cybertrespass** - using cyber-technology to gain or to exceed unauthorized access to:

**Cybervandalism** - using cyber-technology to unleash one or more programs that:

Cyberterrorism
DDoS
Sextortion
Ransomware
Phone Scams
Obscene or offensive content
Online drug trafficking
Online child sexual abuse
THE IMPACT OF CYBERCRIME

$11.7M

22.7%

130

27.4%

Estimated Daily Cybercrime Activity

Regional Distribution of Cybercrime 2017

<table>
<thead>
<tr>
<th>Region (World Bank)</th>
<th>Region GDP (USD, trillions)</th>
<th>Cybercrime Cost (USD, billions)</th>
<th>Cybercrime Loss (% GDP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>20.2</td>
<td>140 to 175</td>
<td>0.69 to 0.87%</td>
</tr>
<tr>
<td>Europe and Central Asia</td>
<td>20.3</td>
<td>160 to 180</td>
<td>0.79 to 0.89%</td>
</tr>
<tr>
<td>East Asia &amp; the Pacific</td>
<td>22.5</td>
<td>120 to 200</td>
<td>0.53 to 0.89%</td>
</tr>
<tr>
<td>South Asia</td>
<td>2.9</td>
<td>7 to 15</td>
<td>0.24 to 0.52%</td>
</tr>
<tr>
<td>Latin America and the Caribbean</td>
<td>5.3</td>
<td>15 to 30</td>
<td>0.28 to 0.57%</td>
</tr>
<tr>
<td>Sub-Saharan Africa</td>
<td>1.5</td>
<td>1 to 3</td>
<td>0.07 to 0.20%</td>
</tr>
<tr>
<td>MENA</td>
<td>3.1</td>
<td>2 to 5</td>
<td>0.06 to 0.16%</td>
</tr>
<tr>
<td>World</td>
<td>$75.8</td>
<td>$445 to $608</td>
<td>0.59 to 0.80%</td>
</tr>
</tbody>
</table>

Source: Accenture, McAfee
CHALLENGES FOR GOVERNMENTS
To maintaining a safe and secure Internet in Asia-Pacific

- Borderless nature of cybercrime
- Emerging Technology & Ease of Criminal Use
- Low cybersecurity awareness
- Difficulty in obtaining cross border cooperation
- Lack of Proper Cyber Legislation
- General lack of specialists and equipment
GOAL:
To better equip governments to handle drugs, crime, terrorism, and corruption-related issues, by maximizing knowledge on these issues among governmental institutions and agencies, and also to maximizing awareness of said matters in public opinion, globally, nationally and at community level.
The three pillars of the **UNODC work programme are:**

- Field-based technical cooperation projects to enhance the capacity of Member States to counteract illicit drugs, crime and terrorism
- Research and analytical work
- Normative work to assist States in the ratification and implementation of the relevant international treaties and the development of domestic legislation
UNODC Global Programme on cybercrime

- UNODC tasked by UN Member States via the Commission on Crime Prevention and Criminal Justice in 2010.
- Published, in draft, a Comprehensive Study on Cybercrime in 2013.
- Established a Global Programme also in 2013.
### UNODC Global Programme on **cybercrime**

**Beneficiary agencies**: Specialized units of the Law Enforcement Agencies, Prosecution and Judiciary

**The objective** to respond to identified needs in developing countries by supporting Member States to prevent and combat cybercrime in a holistic manner through the delivery of crime prevention and criminal justice technical support, based on UNODC assessment protocols and technical assistance tools.

- Normative and Policy
- Capacity building
- Awareness
- International cooperation

---

Cybercrime

Online Child Protection

Digital Forensics
Cybersecurity and Cybercrime activities 2017 - 2018

Number of activities 24
Number of countries involved: 30+
Government officials trained: 500

Types of support:
• Cybercrime and cybersecurity awareness
• Cybersecurity policy strategies and legislation support
• Cyber investigations and prosecution
• Digital forensics
• Understanding digital evidence
• Investigating online child sexual exploitation
• Darknet
• Cryptocurrencies and blockchain
Southeast Asia and Pacific Actions for 2018 - 2019

- Cybercrime threat and readiness study
- Darknet threat research
- Cryptocurrencies
- Cybercrime Roundtable
- Digital Forensics
- Regional Online Child Sexual Exploitation Working Group
Cyber CT
Enhancing capacities to respond to cybercrime and to counter terrorist use of Information and Communications Technology throughout selected ASEAN member states

The objective: Project countries more effectively respond to cybercrime and are able to counter terrorist use of Information and Communications Technology by having increased capacities to detect, investigate and disrupt illicit cybercrime and terrorist activities.

Beneficiary agencies: Prosecution and Law Enforcement agencies of beneficiary countries

Geographical scope: Thailand, Malaysia, Indonesia Philippines

Project Outputs:
- Enhancing Regional Cybercrime Cooperation focused on Countering Terrorist use of Information and Communications Technologies (ICT)
- Enhancing Cyber Terrorism Investigation and cyber intelligence operational capability through Capability Maturity Assessment and Program Enhancement:

Project Activities:
1. Regional Workshop on Terrorism Cybercrime Nexus - one meeting
2. National capacity building training on Cyber Threat Intelligence and Intelligence Community - one per project country
3. Regional training workshops on Cybercrime and Counter Terrorism Policy & Strategy Development – two events

Timeline: March 2018 – March 2019

Funded by the Government of Japan
The objective: Project countries more effectively prevent and counter terrorism financing and money laundering through a better understanding of cryptocurrencies regulatory frameworks and enhanced capacities to identify and investigate crimes involving cryptocurrencies.

Beneficiary agencies: Central Banks, FIUs, Prosecution, Law Enforcement agencies of beneficiary countries.

Geographical scope: Vietnam, Malaysia, Indonesia, Philippines.

Project Outputs:
- Strengthening domestic legal and regulatory frameworks on cryptocurrencies use for AML/CFT as well as come up with practical guide for law enforcement on seizing cryptocurrencies.
- Awareness raised for law and policy makers on evolving cryptocurrencies threats
- Capacity building on effective AML/CFT investigation and prosecution

Project Activities:
1. Southeast Asian Working Group on Cryptocurrencies - one meeting: recommend general cryptocurrency regulations for AML and CFT
2. 4 National Roundtables on Cybercrime and Cryptocurrencies: Raise awareness on risks for AML CFT Money Laundering
3. 4 National Training Courses on Cryptocurrencies and darknet investigations

Timeline: March 2018 – March 2019

Funded by the Government of Japan
**The objective:** of the Programme on Combating Child Sex Offending is to respond to identified needs in Southeast Asian Member States to combat child sexual exploitation in travel and tourism through the delivery of crime prevention and criminal justice technical support

**Beneficiary agencies:** Ministry of Justice, courts, prosecutorial offices, LE agencies (Cambodia, Lao PDR, Viet Nam)

<table>
<thead>
<tr>
<th>Major activities:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Legislation:</strong> Upgrading and regionally harmonizing laws on child sexual abuse offline and online UN CRC</td>
</tr>
<tr>
<td>- Child sexual abuse material</td>
</tr>
<tr>
<td>- Grooming</td>
</tr>
<tr>
<td>- Sanctions, punishment</td>
</tr>
<tr>
<td><strong>Capacity building:</strong> Investigating, prosecuting and adjudicating cases of sexual exploitation of children to police, prosecutors and judges</td>
</tr>
<tr>
<td>- Training manuals and events in English, Khmer, Lao, Thai, Vietnamese</td>
</tr>
<tr>
<td><strong>Cooperation:</strong> Interagency (criminal justice agencies), cross-border and international cooperation</td>
</tr>
<tr>
<td>- Mutual legal assistance, extradition</td>
</tr>
<tr>
<td>- Regional sex offender registry</td>
</tr>
</tbody>
</table>

*Online Child Sexual Exploitation and Abuse*

Enhancing capacities to disrupt and recover illicit cryptocurrency financial flows and terrorist financing and recover such criminal proceeds in selected ASEAN member states

*Funded by the Government of Australia*
Tackling wildlife cybercrime through the use of online platforms and other ICT mediums for illegal selling and trading

The Objective: To establish a functional digital forensics laboratory with appropriate hardware and software in Laos for investigation of wildlife cybercrime and other general cybercrime.

Beneficiary agencies: Lao Police Force

Project Outputs:
- Establishing a functional digital forensics lab
- Provide capacity building trainings to law enforcement agencies, investigators and prosecutors in different phases;
- Discuss the current state of cybersecurity, cybercrime and digital forensics in the country, the challenges and issues

Project Activities
- National Cybercrime Roundtable Discussion
- Establishment of functional Digital Forensics Laboratory
- National Training courses on Digital Forensics for cybercrime and wildlife investigations

Funded by the Government of Norway
Thank You

Alexandru Caciuloiu
Cybercrime Project Coordinator for Southeast Asia and the Pacific

Mobile: +66 61 412 8584
Line id: alex.ctz
WhatsApp: same as mobile
Email: alexandru.caciuloiu@un.org
https://linkedin.com/in/alexandru-caciuloiu-22928543
https://twitter.com/alex_c_unodc